

CERTIFIED COPY OF
PRIORITY DOCUMENT

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

T. Kikuchi

2/21/01

Q63195

10f1

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日

Date of Application:

2000年 2月22日

出願番号

Application Number:

特願2000-050476

出願人

Applicant(s):

日本電気株式会社

JC979 U.S. PTO
09/78566



02/21/01

2001年 1月 5日

特許庁長官
Commissioner,
Patent Office

及川耕造



【書類名】 特許願

【整理番号】 49240018

【提出日】 平成12年 2月22日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 1/00

【発明者】

 【住所又は居所】 東京都港区芝五丁目7番1号 日本電気株式会社内

 【氏名】 菊地 庸之

【特許出願人】

 【識別番号】 000004237

 【氏名又は名称】 日本電気株式会社

【代理人】

 【識別番号】 100084250

 【弁理士】

 【氏名又は名称】 丸山 隆夫

 【電話番号】 03-3590-8902

【手数料の表示】

 【予納台帳番号】 007250

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9303564

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 パケット監視システム、パケット監視方法及びそのプログラム
を記録した記録媒体

【特許請求の範囲】

【請求項 1】 アプリケーションサーバと該アプリケーションサーバを利用
するサービス利用者とを接続する通信路上で送受信されるパケットを監視するパ
ケット監視システムであって、

前記サービス利用者を認証する認証サーバ装置と、

該認証サーバ装置からの依頼により、前記通信路上で送受信されるパケットを
監視するパケット監視装置と、

を有することを特徴とするパケット監視システム。

【請求項 2】 前記認証サーバ装置は、

前記サービス利用者の識別番号、前記サービス利用者を認証するパスワード、
監視するパケットの対象を指定する監視パラメータ、前記パケットの監視方法を
指定する閾値パラメータを含む利用者管理テーブルを記憶している利用者管理情
報記憶手段と、

前記サービス利用者が自装置にログイン／アウトしたタイミングで、前記パケ
ット監視装置に前記パケットの監視の開始／終了を要求する監視要求手段と、

を有することを特徴とする請求項 1 記載のパケット監視システム。

【請求項 3】 前記パケット監視装置は、

前記監視要求手段から監視要求があったとき、前記アプリケーションサーバ及
び前記サービス利用者のいずれかから送信されたパケットの到着時刻を記憶する
到着時刻記憶手段と、

前記監視要求手段から監視要求があったとき、前記到着時刻記憶手段の記憶し
ている到着時間を基に、前記監視パラメータと一致するパケットの到着時刻を監
視し、前記到着間隔に任意の関係が存在するか否かを分析する関連性分析手段と

、
該関連性分析手段による分析の結果、前記任意の関係が存在するとき、前記サ
ービス利用者に通知警告する通知警告手段と、

を有することを特徴とする請求項 2 記載のパケット監視システム。

【請求項 4】 前記認証サーバ装置は、

前記サービス利用者の指示により前記利用者管理テーブルの前記監視パラメータ及び前記閾値パラメータを更新する利用者管理テーブル更新手段をさらに有することを特徴とする請求項 2 または 3 記載のパケット監視システム。

【請求項 5】 前記パケット監視装置は、

前記監視要求手段から転送された前記監視パラメータを記憶する監視パラメータ記憶手段と、

前記監視要求手段から転送された前記閾値パラメータを記憶する閾値パラメータ記憶手段と、

前記監視要求手段からの監視要求の開始／終了のタイミングで、前記監視パラメータ記憶手段及び閾値パラメータ記憶手段を更新するパラメータ更新手段と、

を有することを特徴とする請求項 2 から 4 のいずれか 1 項に記載のパケット監視システム。

【請求項 6】 前記関連性分析手段は、

前記閾値パラメータ記憶手段に閾値パラメータが記憶されているとき、前記到着間隔に任意の関係が存在し、且つ、前記閾値パラメータを超えたか否かを分析し、

前記通知警告手段は、

前記関連性分析手段による分析の結果、前記任意の関係が存在し、且つ、前記閾値パラメータを超えたとき、前記サービス利用者に通知警告することを特徴とする請求項 5 記載のパケット監視システム。

【請求項 7】 アプリケーションサーバと該アプリケーションサーバを利用するサービス利用者とを接続する通信路上で送受信されるパケットを監視するパケット監視方法であって、

前記サービス利用者がログインしたとき、監視するパケットの対象を指定する監視パラメータを含む利用者管理テーブルから、前記監視パラメータを取得するパラメータ取得工程と、

該パラメータ取得工程により取得した監視パラメータと一致するパケットの到着時刻を監視し、前記パケットの到着間隔に任意の関係が存在するか否かを分析する関連性分析工程と、

該関連性分析工程による分析の結果、前記任意の関係が存在するとき、前記サービス利用者に通知警告する通知警告工程と、

を有することを特徴とするパケット監視方法。

【請求項 8】 前記サービス利用者がログアウトしたとき、前記パラメータ分析工程による分析を終了することを特徴とする請求項 7 記載のパケット監視方法。

【請求項 9】 前記利用者管理テーブルは、

前記サービス利用者の識別番号、前記サービス利用者を認証するパスワード、前記パケットの監視方法を指定する閾値パラメータをさらに含み、

前記パラメータ取得工程は、

前記サービス利用者が入力した前記識別番号及び前記パスワードを基に、前記利用者管理テーブルを検索し、

前記利用者管理テーブルに前記監視パラメータが登録されているとき、前記監視パラメータを取得し、

前記利用者管理テーブルに前記閾値パラメータが登録されているとき、前記閾値パラメータを取得することを特徴とする請求項 7 または 8 記載のパケット監視方法。

【請求項 1 0】 前記関連性分析工程は、

前記パラメータ取得工程により前記閾値パラメータを取得したとき、前記パケットの到着間隔に前記任意の関係が存在し、且つ、前記閾値パラメータを越えたか否かを分析し、

前記通知警告工程は、

前記関連性分析工程による分析の結果、前記任意の関係が存在し、且つ、前記閾値パラメータを超えたとき、前記サービス利用者に通知警告することを特徴とする請求項 9 記載のパケット監視方法。

【請求項 1 1】 アプリケーションサーバと該アプリケーションサーバを利

用するサービス利用者とを接続する通信路上で送受信されるパケットを監視するプログラムを記録した記録媒体であって、

前記サービス利用者がログインしたとき、監視するパケットの対象を指定する監視パラメータを含む利用者管理テーブルから、前記監視パラメータを取得するパラメータ取得処理と、

該パラメータ取得処理により取得した監視パラメータと一致するパケットの到着時刻を監視し、前記パケットの到着間隔に任意の関係が存在するか否かを分析する関連性分析処理と、

該関連性分析処理による分析の結果、前記任意の関係が存在するとき、前記サービス利用者に通知警告する通知警告処理と、

をコンピュータに実行させることを特徴とするプログラムを記録した記録媒体。

【請求項 1 2】 前記サービス利用者がログアウトしたとき、前記パラメータ分析処理による分析を終了することを特徴とする請求項 1 1 記載のプログラムを記録した記録媒体。

【請求項 1 3】 前記利用者管理テーブルは、
前記サービス利用者の識別番号、前記サービス利用者を認証するパスワード、
前記パケットの監視方法を指定する閾値パラメータをさらに含み、
前記パラメータ取得処理は、

前記サービス利用者が入力した前記識別番号及び前記パスワードを基に、前記利用者管理テーブルを検索し、

前記利用者管理テーブルに前記監視パラメータが登録されているとき、前記監視パラメータを取得し、

前記利用者管理テーブルに前記閾値パラメータが登録されているとき、前記閾値パラメータを取得することを特徴とする請求項 1 1 または 1 2 記載のプログラムを記録した記録媒体。

【請求項 1 4】 前記関連性分析処理は、
前記パラメータ取得工程により前記閾値パラメータを取得したとき、前記パケットの到着間隔に前記任意の関係が存在し、且つ、前記閾値パラメータを越えた

か否かを分析し、

前記通知警告処理は、

前記関連性分析処理による分析の結果、前記任意の関係が存在し、且つ、前記閾値パラメータを超えたとき、前記サービス利用者に通知警告することを特徴とする請求項 1 3 記載のプログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、従量課金に伴う情報量の機械的なカウントにより生じる不相当なサービス料金、または通信料金の請求を防止するパケット監視システム、パケット監視方法及びそのプログラムを記録した記録媒体に関する。

【0002】

【従来の技術】

近年、電子メールやWebなどのサービスの利用料金は、サービスを提供しているサービスプロバイダへの接続料金や通信事業者に支払う通信料金などで決められている。現在の料金設定はサービスプロバイダ、通信事業者ともに、基本料金に加え、通信時間や距離に依存して行われているが、一部、データ通信ではデータ量に応じた従量課金も採用され始め、今後拡大する傾向にある。

【0003】

このような状況下、インターネット技術の普及と共に、インターネット上で利用できるサービスが多様化している。利用者は、APサーバ（アプリケーションサーバ）から必要な通信ソフトウェアをダウンロードしてサービスを受ける機会が増加しており、サービスの中には独自の通信プロトコルを用い、通信ソフトウェア間で利用者の意図しない制御情報をやりとりするものが現われてきた。例えば、チャットサーバによる定期的な端末の起動確認などである。

【0004】

【発明が解決しようとする課題】

今後拡大する従量課金においては、通信路上で流れるデータ量に応じて課金されるので、利用者の意図しない制御情報にも関わらず課金されてしまうという問

題点がある。それは、情報量の機械的なカウントによるものであり、本来支払うべき料金と実際に請求される料金との不一致を大きくし、利用者はサービスプロバイダに対する不信感を募らせ、ひいてはサービスプロバイダとの契約を解除することにつながる可能性もある。

【 0 0 0 5 】

本発明はかかる問題点に鑑みなされたものであり、利用者の意図しない制御情報にも関わらず課金されてしまうという事態を防止し、利用者が受領したサービスに見合った適正な課金を行う機能を有するパケット監視システム、パケット監視方法及びそのプログラムを記録した記録媒体を提供することを目的とする。

【 0 0 0 6 】

【課題を解決するための手段】

かかる目的を達成するために、請求項 1 記載の発明は、アプリケーションサーバと該アプリケーションサーバを利用するサービス利用者とを接続する通信路上で送受信されるパケットを監視するパケット監視システムであって、サービス利用者を認証する認証サーバ装置と、該認証サーバ装置からの依頼により、通信路上で送受信されるパケットを監視するパケット監視装置と、を有することを特徴とする。

【 0 0 0 7 】

請求項 2 記載の発明は、請求項 1 記載の発明において、認証サーバ装置は、サービス利用者の識別番号、サービス利用者を認証するパスワード、監視するパケットの対象を指定する監視パラメータ、パケットの監視方法を指定する閾値パラメータを含む利用者管理テーブルを記憶している利用者管理情報記憶手段と、サービス利用者が自装置にログイン／アウトしたタイミングで、パケット監視装置にパケットの監視の開始／終了を要求する監視要求手段と、を有することを特徴とする。

【 0 0 0 8 】

請求項 3 記載の発明は、請求項 2 記載の発明において、パケット監視装置は、監視要求手段から監視要求があったとき、アプリケーションサーバ及びサービス利用者のいずれかから送信されたパケットの到着時刻を記憶する到着時刻記憶手

段と、監視要求手段から監視要求があったとき、到着時刻記憶手段の記憶している到着時間を基に、監視パラメータと一致するパケットの到着時刻を監視し、到着間隔に任意の関係が存在するか否かを分析する関連性分析手段と、該関連性分析手段による分析の結果、任意の関係が存在するとき、サービス利用者に通知警告する通知警告手段と、を有することを特徴とする。

【 0 0 0 9 】

請求項 4 記載の発明は、請求項 2 または 3 記載の発明において、認証サーバ装置は、サービス利用者の指示により利用者管理テーブルの監視パラメータ及び閾値パラメータを更新する利用者管理テーブル更新手段をさらに有することを特徴とする。

【 0 0 1 0 】

請求項 5 記載の発明は、請求項 2 から 4 のいずれか 1 項に記載の発明において、パケット監視装置は、監視要求手段から転送された監視パラメータを記憶する監視パラメータ記憶手段と、監視要求手段から転送された閾値パラメータを記憶する閾値パラメータ記憶手段と、監視要求手段からの監視要求の開始／終了のタイミングで、監視パラメータ記憶手段及び閾値パラメータ記憶手段を更新するパラメータ更新手段と、を有することを特徴とする。

【 0 0 1 1 】

請求項 6 記載の発明は、請求項 5 記載の発明において、関連性分析手段は、閾値パラメータ記憶手段に閾値パラメータが記憶されているとき、到着間隔に任意の関係が存在し、且つ、閾値パラメータを超えたか否かを分析し、通知警告手段は、関連性分析手段による分析の結果、任意の関係が存在し、且つ、閾値パラメータを超えたとき、サービス利用者に通知警告することを特徴とする。

【 0 0 1 2 】

請求項 7 記載の発明は、アプリケーションサーバと該アプリケーションサーバを利用するサービス利用者とを接続する通信路上で送受信されるパケットを監視するパケット監視方法であって、サービス利用者がログインしたとき、監視するパケットの対象を指定する監視パラメータを含む利用者管理テーブルから、監視パラメータを取得するパラメータ取得工程と、該パラメータ取得工程により取得

した監視パラメータと一致するパケットの到着時刻を監視し、パケットの到着間隔に任意の関係が存在するか否かを分析する関連性分析工程と、該関連性分析工程による分析の結果、任意の関係が存在するとき、サービス利用者に通知警告する通知警告工程と、を有することを特徴とする。

【 0 0 1 3 】

請求項 8 記載の発明は、請求項 7 記載の発明において、サービス利用者がログアウトしたとき、パラメータ分析工程による分析を終了することを特徴とする。

【 0 0 1 4 】

請求項 9 記載の発明は、請求項 7 または 8 記載の発明において、利用者管理テーブルは、サービス利用者の識別番号、サービス利用者を認証するパスワード、パケットの監視方法を指定する閾値パラメータをさらに含み、パラメータ取得工程は、サービス利用者が入力した識別番号及びパスワードを基に、利用者管理テーブルを検索し、利用者管理テーブルに監視パラメータが登録されているとき、監視パラメータを取得し、利用者管理テーブルに閾値パラメータが登録されているとき、閾値パラメータを取得することを特徴とする。

【 0 0 1 5 】

請求項 1 0 記載の発明は、請求項 9 記載の発明において、関連性分析工程は、パラメータ取得工程により閾値パラメータを取得したとき、パケットの到着間隔に任意の関係が存在し、且つ、閾値パラメータを越えたか否かを分析し、通知警告工程は、関連性分析工程による分析の結果、任意の関係が存在し、且つ、閾値パラメータを超えたとき、サービス利用者に通知警告することを特徴とする。

【 0 0 1 6 】

請求項 1 1 記載の発明は、アプリケーションサーバと該アプリケーションサーバを利用するサービス利用者とを接続する通信路上で送受信されるパケットを監視するプログラムを記録した記録媒体であって、サービス利用者がログインしたとき、監視するパケットの対象を指定する監視パラメータを含む利用者管理テーブルから、監視パラメータを取得するパラメータ取得処理と、該パラメータ取得処理により取得した監視パラメータと一致するパケットの到着時刻を監視し、パ

ケットの到着間隔に任意の関係が存在するか否かを分析する関連性分析処理と、該関連性分析処理による分析の結果、任意の関係が存在するとき、サービス利用者に通知警告する通知警告処理と、をコンピュータに実行させることを特徴とする。

【 0 0 1 7 】

請求項 1 2 記載の発明は、請求項 1 1 記載の発明において、サービス利用者がログアウトしたとき、パラメータ分析処理による分析を終了することを特徴とする。

【 0 0 1 8 】

請求項 1 3 記載の発明は、請求項 1 1 または 1 2 記載の発明において、利用者管理テーブルは、サービス利用者の識別番号、サービス利用者を認証するパスワード、パケットの監視方法を指定する閾値パラメータをさらに含み、パラメータ取得処理は、サービス利用者が入力した識別番号及びパスワードを基に、利用者管理テーブルを検索し、利用者管理テーブルに監視パラメータが登録されているとき、監視パラメータを取得し、利用者管理テーブルに閾値パラメータが登録されているとき、閾値パラメータを取得することを特徴とする。

【 0 0 1 9 】

請求項 1 4 記載の発明は、請求項 1 3 記載の発明において、関連性分析処理は、パラメータ取得工程により閾値パラメータを取得したとき、パケットの到着間隔に任意の関係が存在し、且つ、閾値パラメータを越えたか否かを分析し、通知警告処理は、関連性分析処理による分析の結果、任意の関係が存在し、且つ、閾値パラメータを超えたとき、サービス利用者に通知警告することを特徴とする。

【 0 0 2 0 】

【発明の実施の形態】

以下、本発明の実施の形態を添付図面を参照しながら詳細に説明する。

【 0 0 2 1 】

図 1 は、本発明のパケット監視システムの基本構成を示すブロック図である。図 1 において、サービス利用者は、サービスプロバイダ 4 との間でサービス料金

や監視方法について契約を交わし、データ情報端末 1 を利用して、有線／無線通信網 2、通信路 3、サービスプロバイダ 4、インターネット 7 を介して、A P サーバ 8 からサービスやコンテンツ情報を授受する。ここで、パケットとは、ユーザデータと、ヘッダ（送受信先アドレスやサービス識別子、チェックサム、ユーザデータやヘッダのサイズ等の制御情報）とから構成されるインターネット転送プロトコルの基本転送単位ブロックを指す。

【 0 0 2 2 】

サービスプロバイダ 4 は、サービス利用者を認証する認証サーバ 5、通信路 3 上で送受信されるパケットを監視するパケット監視装置 6 を有する。サービスプロバイダ 4 には、有線や無線による通信路を提供する通信事業者も含まれる。認証サーバ 5 は、利用者管理テーブルを格納している利用者管理メモリ 9、利用者からの指示により利用者管理メモリ 9 の内容を更新する管理メモリ更新手段 1 0 及びサービス利用者が認証サーバ 5 にログイン／アウトしたタイミングでパケット監視装置 6 に対して、監視の開始／終了を要求する監視要求手段 1 1 を有する。

【 0 0 2 3 】

管理メモリ更新手段 1 0 は、サービスプロバイダ 4 が契約時に提示した監視パラメータ、閾値パラメータを基に利用者管理メモリ 9 の内容を更新する。あるいは、サービスプロバイダ 4 が自身で提供している World-Wide-Web のホームページ上において、サービス利用者が入力した監視パラメータ、閾値パラメータを基に利用者管理メモリ 9 の内容を更新する。あるいは、サービスプロバイダ 4 が提供するデータ情報端末 1 上で動作するパラメータ設定プログラム上において、サービス利用者が入力した監視パラメータ、閾値パラメータを基に利用者管理メモリ 9 の内容を更新する。

【 0 0 2 4 】

パケット監視装置 6 は、監視パラメータを格納しておく監視パラメータメモリ 1 2、閾値パラメータを格納しておく閾値パラメータメモリ 1 3、データ情報端末 1 もしくは A P サーバ 8 から送信されたパケットの到着時刻を格納しておく到着時刻メモリ 1 4、認証サーバ 5 から監視要求の開始／終了を受けたタイミング

でパラメータメモリ 1 2、1 3 を更新するパラメータ更新手段 1 5、到着間隔の関連性を分析する関連性分析手段 1 6 及び利用者に通知／警告を行う通知／警告手段 1 7 を有する。

【 0 0 2 5 】

通知／警告手段 1 7 は、サービスプロバイダ 4 が書面や掲示板にて利用者に通知／警告を行う。あるいは、サービスプロバイダ 4 が提供するサービスが使用している通信プロトコルに通知／警告を添付して利用者に通知／警告を行う。あるいは、サービスプロバイダ 4 がデータ情報端末 1 上で動作可能な通知／警告プログラムを送り付けることにより利用者に通知／警告を行う。

【 0 0 2 6 】

監視パラメータは、送受信先アドレスと、サービス識別子と、ユーザデータ内の任意データ列と、チェックサムのいずれか、あるいはその組み合わせとする。送受信先アドレスとは、パケットを届けるための宛て先や送り元を示す制御情報である。サービス識別子とは、A P サーバ 8 が利用者に提供するサービス（例えば、電子メールなど）を識別するための制御情報である。チェックサムとは、ユーザデータやヘッダが転送の際に壊れていないかどうかをチェックするための制御情報であり、ユーザデータやヘッダが等しい場合、チェックサムの情報も等しいものとする。

【 0 0 2 7 】

監視する対象とその組み合わせ（監視パラメータ）の一例を図 2 に示す。図 2 に示す監視パラメータは、送受信先アドレスとサービス識別子との組、送受信先アドレスとユーザデータ内の任意位置から始まる任意サイズのデータ列（以下、任意データ列とする。）との組、送受信先アドレスとサービス識別子と任意データ列との組、チェックサムのいずれかからなる。監視パラメータ A は、例えば、データ情報端末 1 から電子メールサービスを提供する A P サーバ 8 へ定期的に受信メール確認パケットが流れているか否か、チャットサービスを提供する A P サーバ 8 からデータ情報端末 1 へ定期的に端末の起動確認パケットが流れているか否かを監視するためのパラメータとなりうる。

【 0 0 2 8 】

閾値パラメータは、監視パラメータが一致してからの継続時間、連続して一致した回数、一致してから送受信されたユーザデータあるいはヘッダサイズ、一致してからの利用料金、通信路 3 上のトラフィック量のいずれか、あるいはその組み合わせとする。閾値パラメータの一例を図 3 に示す。図 3 に示す閾値パラメータは、監視パラメータが一致してからの継続時間（閾値 A）、連続して一致した回数（閾値 B）、一致してから送受信されたユーザデータヘッダあるいはヘッダサイズ（閾値 C）、一致してからの利用料金（閾値 D）のいずれかからなる。

【 0 0 2 9 】

利用者管理メモリ 9 に記憶されている利用者管理テーブルの一例を図 4 に示す。利用者管理テーブルは、契約を交わした利用者の識別番号、利用者を認証するためのパスワード、監視パラメータ、閾値パラメータ及びパケット監視中か否かを示すフラグから構成される。

【 0 0 3 0 】

次に、本発明のパケット監視システムの動作について説明する。サービス利用者が、サービスプロバイダ 4 との間でサービス料金や監視方法について契約を交わし、データ情報端末 1 を利用し、有線／無線通信網 2、通信路 3、サービスプロバイダ 4、インターネット 7 を介して、AP サーバ 8 からサービスやコンテンツ情報を授受し、サービスプロバイダ 4 が、サービス利用者を認証する認証サーバ 5、通信路 3 上で送受信されるパケットを監視するパケット監視装置 6 を有するシステム上で、サービス利用者が認証サーバにログイン／アウトしたタイミングで、パケット監視装置 6 の監視パラメータメモリ 1 2 及び閾値パラメータメモリ 1 3 の内容を通信／更新する動作を図 5 に示すフローチャートを用いて説明する。

【 0 0 3 1 】

図 5 において、監視要求手段 1 1 は、サービス利用者が認証サーバ 5 にログインしたタイミングで、利用者管理メモリ 9 からログインした利用者を検索する（ステップ S 1）。監視要求手段 1 1 は、サービス利用者に指示された監視パラメータが存在するか否かを確認する（ステップ S 2）。当該監視パラメータが存在する場合は（ステップ S 2／YES）、利用者管理メモリ 9 に保持されている監

視パラメータと閾値パラメータとを読み込む（ステップ S 4）。読み込んだ 2 つのパラメータを引数として、パケットの監視開始をパラメータ更新手段 1 5 に要求する（ステップ S 5）。ステップ S 2 において、サービス利用者に指示された監視パラメータが存在しない場合は（ステップ S 3 / NO）、パケットの監視は行わない（ステップ S 3）。

【 0 0 3 2 】

パラメータ更新手段 1 5 は、渡された 2 つのパラメータを各々、監視パラメータメモリ 1 2、閾値パラメータメモリ 1 3 に格納する（ステップ S 6）。パラメータ更新手段 1 5 は、格納した旨を監視要求手段 1 1 に通知する（ステップ S 7）。

【 0 0 3 3 】

監視要求手段 1 1 は、パラメータ更新手段 1 5 から通知を受けると利用者管理メモリ 9 のログインした利用者に対応するフラグをセットする（ステップ S 8）。パラメータ更新手段 1 5 は、関連性分析手段 1 6 に監視パラメータで示されたパケットの到着間隔の関連性を分析するよう要求する（ステップ S 9）。

【 0 0 3 4 】

次に、監視要求手段 1 1 は、サービス利用者が認証サーバ 5 からログアウトしたタイミングで、利用者管理メモリ 9 からログアウトした利用者を検索する（ステップ S 1 0）。当該利用者に対応するフラグがセットされているか否かを確認する（ステップ S 1 1）。フラグがセットされている場合は（ステップ S 1 1 / YES）、監視要求手段 1 1 は、パラメータ更新手段 1 5 に監視パラメータ及び閾値パラメータを引数としてパケットの監視終了を要求する（ステップ S 1 3）。ステップ S 1 1 において、フラグがセットされていない場合は（ステップ S 1 1 / NO）、何も処理しない（ステップ S 1 2）。

【 0 0 3 5 】

パケットの監視終了の要求を受けたパラメータ更新手段 1 5 は、関連性分析手段 1 6 に監視パラメータで示されたパケットの到着間隔の関連性の分析を終了するよう要求する（ステップ S 1 4）。パラメータ更新手段 1 5 は、監視パラメータメモリ 1 2、閾値パラメータメモリ 1 3 からパラメータを消去する（ステップ

S 1 5)。パラメータ更新手段 1 5 は、当該パラメータを消去した旨を監視要求手段 1 1 に通知する（ステップ S 1 6）。当該通知を受けた監視要求手段 1 1 は、利用者管理メモリ 9 のログアウトした利用者に対応するフラグをクリアする（ステップ S 1 7）。

【 0 0 3 6 】

次に、パケットの到着間隔の関連性を分析し、パケット送受信による問題があると判断した場合、通知／警告手段 1 7 に通知する動作を図 6 に示すフローチャートを用いて説明する。到着時刻メモリ 1 4 には、データ通信端末 1、または A P サーバ 8 からパケットが到着したタイミングで、パケットが到着した時刻、パケット送信元のアドレス、パケット受信先のアドレス、任意データ列、チェックサム、ユーザデータサイズ、ヘッダデータサイズが随時書き込まれるものとする。

【 0 0 3 7 】

図 6 において、関連性分析手段 1 6 は、パラメータ更新手段 1 5 から関連性分析開始要求を受け取る（ステップ S 9）。関連性分析手段 1 6 は、当該関連性分析開始要求を受け取るとカウンタをクリアする（ステップ S 2 1）。関連性分析手段 1 6 は、監視パラメータメモリ 1 2 を参照して監視パラメータの有無を確認する（ステップ S 2 2）。監視パラメータが存在しない場合は（ステップ S 2 2 / N O）、関連性の分析を終了する（ステップ S 2 3）。監視パラメータが存在する場合は（ステップ S 2 2 / Y E S）、関連性分析手段 1 6 は、閾値パラメータメモリ 1 3 を参照して閾値パラメータの有無を確認する（ステップ S 2 4）。

【 0 0 3 8 】

閾値パラメータが存在する場合は（ステップ S 2 4 / Y E S）、関連性分析手段 1 6 は、閾値確認フラグをセットする（ステップ S 2 5）。フラグをセットしたら到着時刻メモリ 1 4 を参照して監視パラメータに該当するパケットの有無を確認する（ステップ S 2 6）。ステップ S 2 4 に戻り、閾値パラメータが存在しない場合は（ステップ S 2 4 / N O）、到着時刻メモリ 1 4 を参照して監視パラメータに該当するパケットの有無を確認する（ステップ S 2 6）。

【 0 0 3 9 】

パケットが存在しない場合は（ステップ S 2 6 / N O）、ステップ S 2 2 に戻る。パケットが存在する場合は（ステップ S 2 6 / Y E S）、関連性分析手段 1 6 は、カウンタをインクリメントする（ステップ S 2 7）。関連性分析手段 1 6 は、カウンタが 2 以上か否かを確認する（ステップ S 2 8）。

【 0 0 4 0 】

カウンタが 2 未満の場合は（ステップ S 2 8 / N O）、ステップ S 2 2 に戻る。カウンタが 2 以上の場合は（ステップ S 2 8 / Y E S）、関連性分析手段 1 6 は、該当するパケットの到着時間間隔に関連性があるか否かを分析する（ステップ S 2 9）。

【 0 0 4 1 】

ステップ S 2 9 において、関連性がない場合は（ステップ S 2 9 / N O）、ステップ S 2 2 に戻る。関連性がある場合は（ステップ S 2 9 / Y E S）、関連性分析手段 1 6 は、閾値確認フラグがセットされているか否かを確認する（ステップ S 3 0）。該当するパケットの到着時間間隔の関連性は、X 秒間隔で到着している。あるいは、X 秒と Y 秒間隔が交互に繰り返されている。

【 0 0 4 2 】

ステップ S 3 0 において、閾値確認フラグがセットされていない場合は（ステップ S 3 0 / N O）、関連性分析手段 1 6 は、通信路 3 上に利用者が意図しないパケット、または利用者が故意に送信したパケットが流れているものと判断し、通知／警告手段 1 7 に通知する（ステップ S 3 1）。通知後、ステップ S 2 1 に戻る。ステップ S 3 0 において、閾値確認フラグがセットされている場合は（ステップ S 3 0 / Y E S）、閾値を超えたか否かを確認する（ステップ S 3 2）。

【 0 0 4 3 】

閾値を越えていない場合は（ステップ S 3 2 / N O）、ステップ S 2 2 に戻る。閾値を越えた場合は（ステップ S 3 2 / Y E S）、関連性分析手段 1 6 は、通信路 3 上に利用者が意図しないパケット、または利用者が故意に送信したパケットが流れているものと判断し、通知／警告手段 1 7 に通知する（ステップ S 3 3）。

）。通知後、ステップ S 2 1 に戻る。

【 0 0 4 4 】

【発明の効果】

以上の説明から明らかなように、本発明によれば、従量課金に伴う情報量の機械的なカウントにより生じる不相当なサービス料金、または通信料金の請求を防止することができる。

【 0 0 4 5 】

また、サービス利用者が主に利用するサービスを考慮してパラメータを設定し、通知／警告を受けるべきパケットの種類を特定することにより、パケット監視装置における関連性分析の処理効率を向上させることができる。

【図面の簡単な説明】

【図 1】

本発明の実施の形態におけるパケット監視システムの構成を示すブロック図である。

【図 2】

監視パラメータの一例を示した図である。

【図 3】

閾値パラメータの一例を示した図である。

【図 4】

利用者管理テーブルの一例を示した図である。

【図 5】

本発明の実施の形態における監視要求手段 1 1、パラメータ更新手段 1 5 及び関連性分析手段 1 6 の動作を説明するためのフローチャートである。

【図 6】

本発明の実施の形態におけるパラメータ更新手段 1 5、関連性分析手段 1 6 及び通知／警告手段 1 7 の動作を説明するためのフローチャートである。

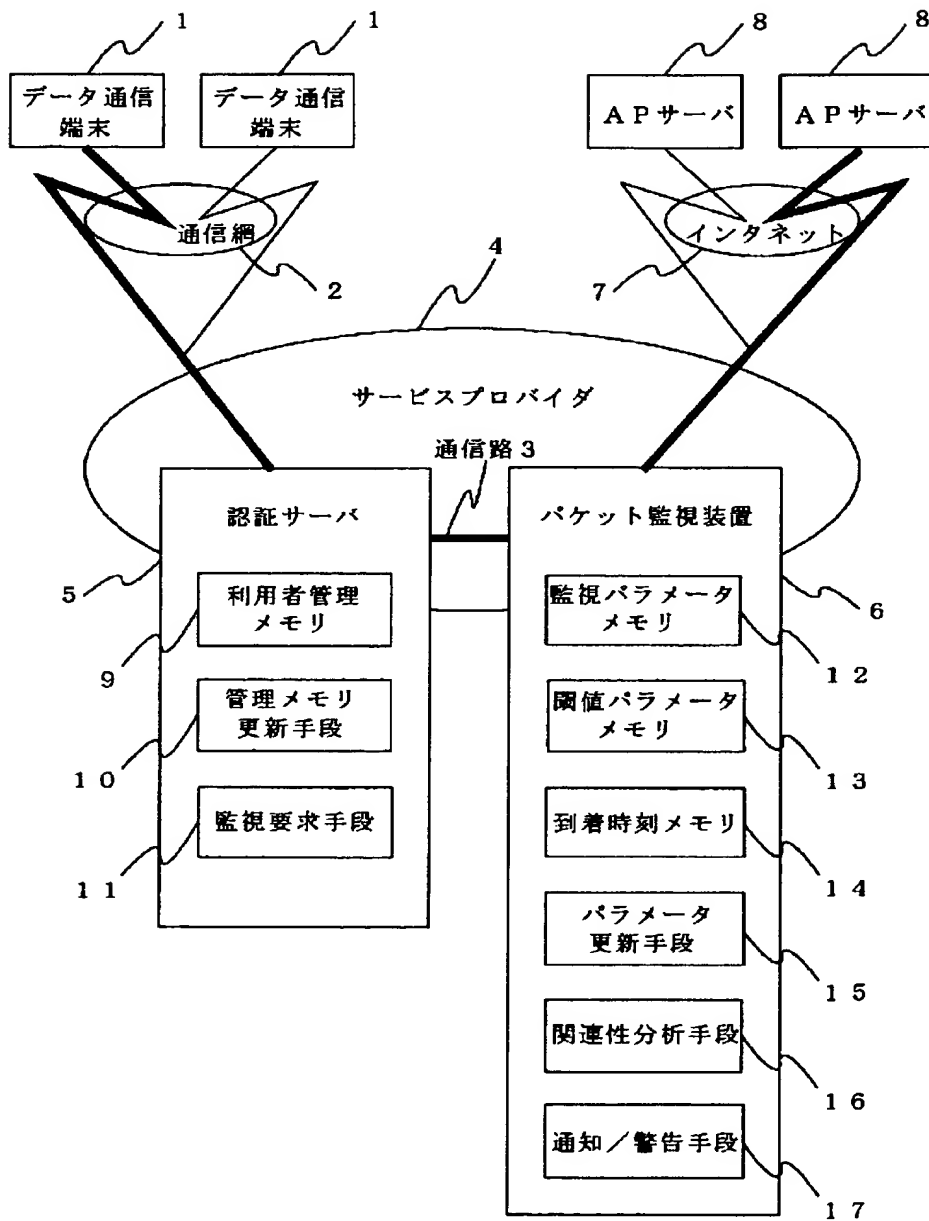
【符号の説明】

- 1 データ通信端末
- 2 通信網

- 3 通信路
- 4 サービスプロバイダ
- 5 認証サーバ
- 6 パケット監視装置
- 7 インタネット
- 8 A Pサーバ
- 9 利用者管理メモリ
- 1 0 管理メモリ更新手段
- 1 1 監視要求手段
- 1 2 監視パラメータメモリ
- 1 3 閾値パラメータメモリ
- 1 4 到着時刻メモリ
- 1 5 パラメータ更新手段
- 1 6 関連性分析手段
- 1 7 通知／警告手段

【書類名】 図面

【図 1】

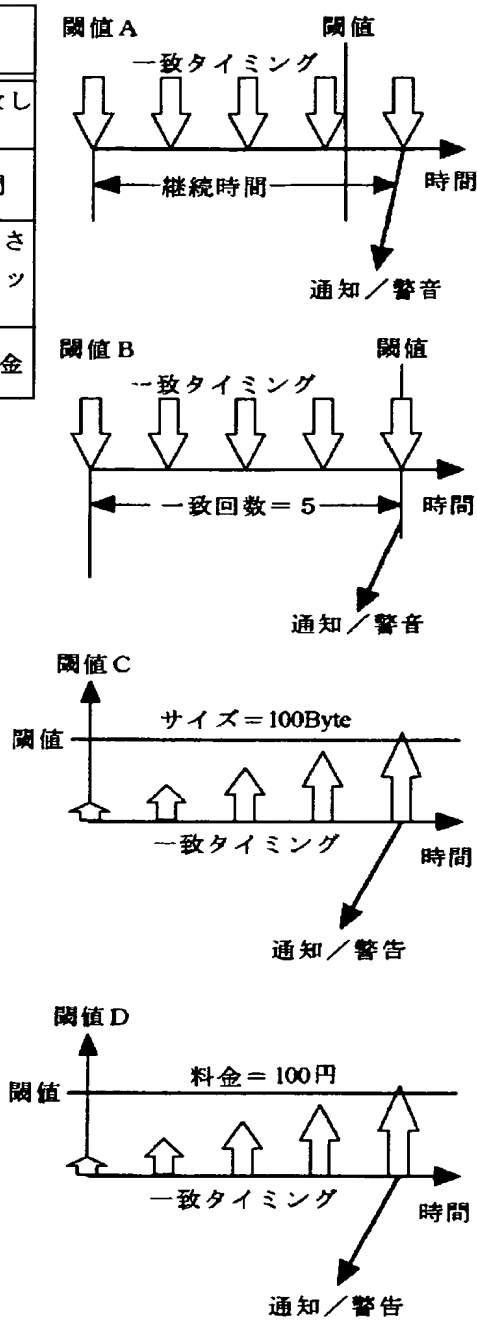


【図 2】

監視パラメータ 監視対象	パラメータ A	パラメータ B	パラメータ C	パラメータ D
送受信先 アドレス	●	●	●	
サービス 識別子	●		●	
任意データ列		●	●	
チェックサム				●

【図 3】

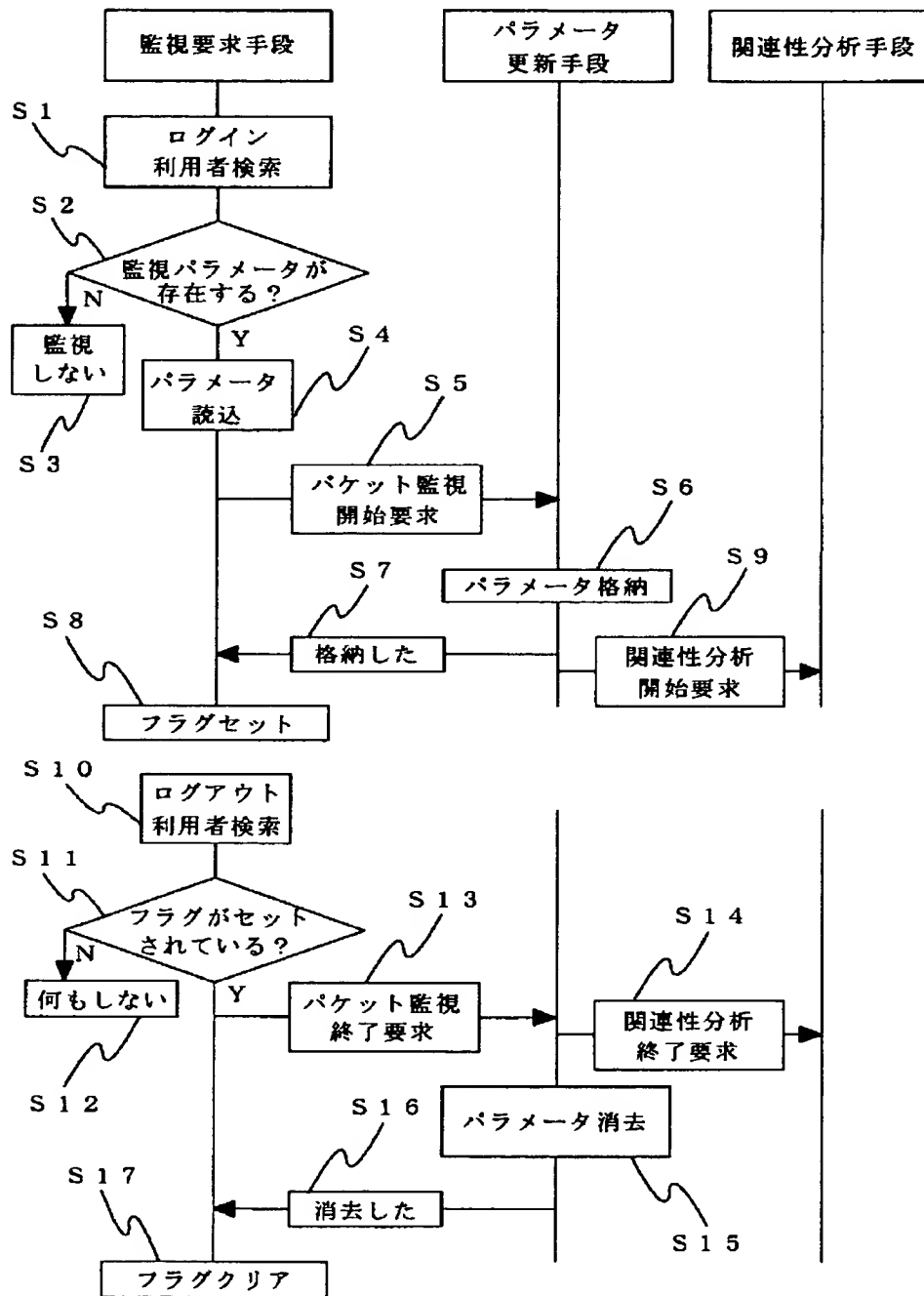
閾値 パラメータ	説明
閾値 A	監視パラメータが一致し てからの継続時間
閾値 B	連続して一致した時間
閾値 C	一致してからの送受信さ れたユーザデータ、ヘッ ダサイズ
閾値 D	一致してからの利用料金



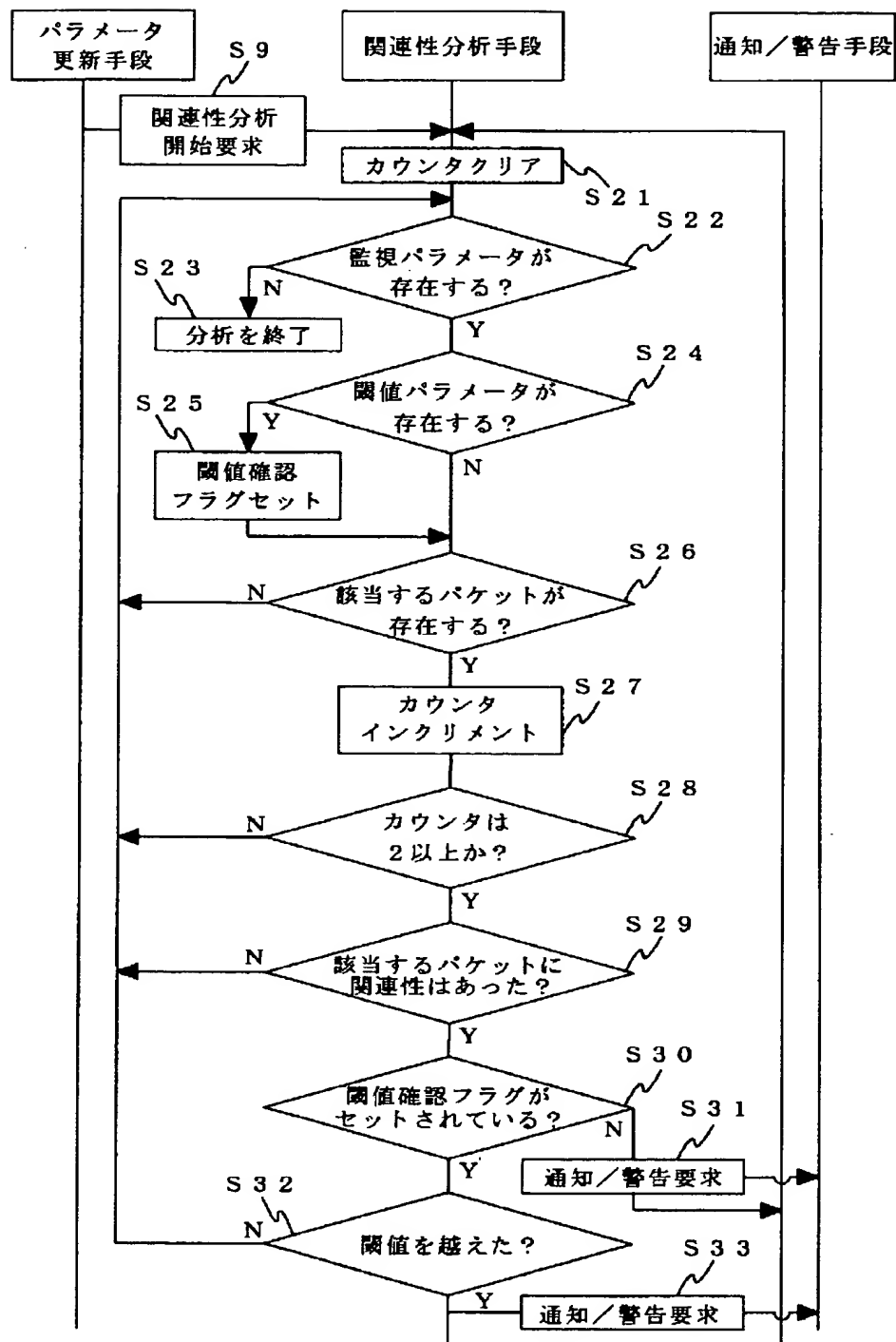
【図 4】

テーブル I D	利用者 識別番号	パスワード	監視 パラメータ	閾値 パラメータ	メモリ アドレス
1	I D 1 2 3 4	X X X X	A	A	0 x 1 0 0 0
2	I D 5 6 7 8	Y Y Y Y	B	C	0 x 2 0 0 0
3	I D 9 9 9 9	Z Z Z Z	D	E	0 x 3 0 0 0

【図 5】



【図6】



【書類名】 要約書

【要約】

【課題】 従量課金に伴う情報量の機械的なカウントにより生じる不相当なサービス料金、または通信料金の請求を防止するパケット監視システム、パケット監視方法及びそのプログラムを記録した記録媒体を提供する。

【解決手段】 サービス利用者がログインしたとき、監視パラメータを構成要素として持つ利用者管理テーブルを検索して、当該サービス利用者に対応する監視パラメータを取得して、当該監視パラメータと一致するパケットの到着時刻を常時監視し、到着間隔に任意の関係が存在する場合、通信路上に利用者が意図しないパケット、又は利用者が故意に送信したパケットが流れているものと判断し、サービス利用者に通知／警告することにより実行する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000004237]

1. 変更年月日	1990年 8月29日
[変更理由]	新規登録
住 所	東京都港区芝五丁目7番1号
氏 名	日本電気株式会社